CS 70 Discrete Mathematics and Probability Theory
Spring 2025 Rao Midterm

PRINT Your Name: _____, _____
(last) (first)

PRINT Your Student ID: _____

PRINT Your Exam Room: _____

SID of the person sitting to your left: _____

SID of the person sitting to your right: _____

SID of the person sitting in front of you: _____

SID of the person sitting behind you: _____

Read This.

- There will be no clarifications. We will correct any mistakes post-exam in as fair a manner as possible. Please just answer the question as best you can and move on even if you feel it is a mistake.
- There are lots of problems to get points from. Do not get stuck. This is good advice anyway. In fact, we repeat it below.
- Anything written outside the boxes provided will not be graded.

Advice.

- The questions vary in difficulty. In particular, the exam is not in the order of difficulty and quite accessible short answer and proof questions are late in the exam. All blanks are worth 3 points each unless otherwise specified. No points will be given for a blank answer, and there will be no negative points on the exam. **So do really scan over the exam.**
- The question statement is your friend. Reading it carefully is a tool to get to your "rational place".
- You may consult only *one sheet of notes on both sides*. Apart from that, you may not look at books, notes, ChatGPT, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture, unless otherwise stated. That is, if we ask you to prove a statement, prove it from basic definitions, e.g., "$d \mid x$ means $x = kd$ for some integer k" is a definition.**
- There are a total of 237 points on this exam, with 12 total questions.

1. Pledge.

Berkeley Honor Code: As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.

In particular, I acknowledge that:

- I alone am taking this exam. Other than with the course staff, I will not have any verbal, written, or electronic communication about the exam with anyone else while I am taking the exam or while others are taking the exam.
- I will not refer to any books, notes, or online sources of information while taking the exam, other than what the instructor has allowed.
- I will not take screenshots, photos, or otherwise make copies of exam questions to share with others.

SIGN Your Name: _____

2. Warmup

(1 point) How many TAs does CS70 have this semester?

3. Propositions

1. Let P, Q, and R be propositions. Determine whether the following statements are true or false.

   (a) $(\neg P \wedge R) \vee (\neg P \wedge Q) \equiv \neg P \wedge (R \vee Q)$.

   ◯ True ◯ False

   (b) $(P \wedge Q) \wedge (\neg P \vee \neg Q) \equiv P \wedge \neg P$.

   ◯ True ◯ False

   (c) $((P \implies Q) \wedge (P \implies \neg Q)) \equiv \neg P$.

   ◯ True ◯ False

   (d) $((P \implies R) \wedge (P \implies \neg R)) \equiv \neg R$.

   ◯ True ◯ False

2. Let $P(n)$ and $Q(n)$ be predicates on $n \in \mathbb{N}$.

   (a) What is the negation of $(\forall n \in N)(P(n))$? (Your answer must not use $\forall$.)

   (b) Is the following statement true for all propositions $P(n)$?

   $$[\neg(\forall n \in \mathbb{N})(P(n)) \wedge P(0)] \implies (\exists n \in \mathbb{N})(P(n) \wedge \neg P(n+1)).$$

   ◯ Always True ◯ Possibly False

   (c) $(\forall n \in \mathbb{N})(Q(n) \wedge P(n)) \equiv (\forall n \in \mathbb{N})(Q(n)) \wedge (\forall n \in \mathbb{N})(P(n))$

   ◯ Always True ◯ Possibly False

   (d) $(\forall n \in \mathbb{N})(Q(n) \implies P(n)) \equiv (\forall n \in \mathbb{N})(\neg Q(n)) \vee (\forall n \in \mathbb{N})(P(n))$

   ◯ Always True ◯ Possibly False

4. Short proofs or counterexample.

1. (5 points) Prove the following statement or give a counterexample. Given 3 people, where each person likes exactly one other person, there is always someone that no one likes.

2. (10 points) Let (a,b,c) be a *primitive right triangle*, meaning that $a,b,c > 0$ are integers that satisfy the Pythagorean theorem

$$a^2 + b^2 = c^2,$$

and all three values are coprime.

Prove that the length of the hypotenuse c of any *primitive right triangle* must be odd.

5. Induction.

(15 points) Prove that $\forall n \in \mathbb{N}$, we have $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

Hint: You may use the fact that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. *You should not need to expand* $(n+1)^3$.

6. Stable Matching.

In the following parts, we consider stable matching instances with n jobs and n candidates.

1. Out of all possible stable matching instances, what is the maximum number of rogue couples in any pairing? (Your answer should be in terms of n.)

2. If a stable matching is optimal for a job, it is pessimal for the candidate it is paired with.

   ◯ True ◯ False

3. In the propose and reject algorithm with jobs proposing, if a candidate C rejects $n-1$ jobs, then C is paired with their favorite job.

   ◯ True ◯ False

4. In the propose and reject algorithm with jobs proposing, if a job J is rejected by candidate C and a different job J' is paired with C, then J ends up with a worse ranked candidate in their ordering than J'. (The rank of a candidate is the position in the job's list. It's worse if it is lower on their preference list.)

   ◯ True ◯ False

5. (a) In a stable matching instance, if job J and candidate C each put each other at the top of their respective preference lists, then J must be paired with C in every stable matching.

   ◯ True ◯ False

   (b) (4 points) Prove that for every $n \geq 2$, there exists a stable matching instance with **only one** stable matching.

(c) (5 points) Prove that for every $n \geq 2$, there exists a stable matching instance with **exactly two** stable matchings.

7. Graphs

All graphs are simple and undirected unless otherwise specified.

1. Consider a connected planar graph G with a planar drawing with f faces, v vertices, and e edges.

   (a) Suppose $v \geq 3$. What is the maximum number of faces in G, in terms of v?

   Now, suppose every cycle in G has at least g edges.

   (b) The number of edges in G is at most

   $$\frac{g}{g-2}v - \_\_\_\_\_.$$

   (Give a tight bound.)

   (c) (5 points) Prove that if g is at least 6, then the graph is 3 colorable.

2. Recall that the complement of a graph $G = (V, E)$ is a graph $\overline{G} = (V, \overline{E})$ on the same vertex set V with an edge $(u, v) \in \overline{E}$ if and only if $(u, v) \notin E$.

   (a) Let G be a tree on n vertices. How many edges are in the complement of G?

(b) Let G be a d-dimensional hypercube. How many edges are in the complement of G?

3. The *double* of a graph $G = (V, E)$ is the graph G', constructed by making a copy of the original graph (including all edges), and connecting corresponding vertices across the two copies with an edge. Formally, $G' = (V \cup V', E')$ where $v' \in V'$ corresponds one-to-one to each $v \in V$, and $E' = \{(v, v') \mid v \in V\} \cup \{(u, v), (u', v') \mid (u, v) \in E\}$.

(a) In a graph G with n vertices and m edges, how many edges are in its double, G'? (Your answer should be in terms of n and m.)

(b) If G is bipartite, then G' is bipartite.

◯ True ◯ False

(c) The d-dimensional hypercube is the graph formed by doubling a k-dimensional hypercube _____ times. (You may assume that $k < d$.)

(d) If one doubles a n-vertex tree, what is the minimum number edges that must be removed from the doubled graph to ensure that it is acyclic?

(e) If a graph is $c \geq 2$ vertex colorable, then its doubled graph is _____ vertex colorable. (Fill in the blank with the smallest value, possibly in terms of c and/or the number of vertices n and edges m in the original graph.)

(f) If a graph contains a Hamiltonian cycle and has at least two vertices, then its doubled graph also contains a Hamiltonian cycle.

◯ True ◯ False

(g) If a graph contains an Eulerian tour and has at least two vertices, then its doubled graph also contains an Eulerian tour.

◯ True ◯ False

8. Graph: proof.

(8 points) Let $G = (V, E)$ be a disconnected graph. Prove that its complement $\overline{G} = (V, \overline{E})$ is connected. (Recall that the complement of a graph is defined such that for $u, v \in V$, $(u, v) \in E$, if and only if $(u, v) \notin \overline{E}$.)

9. Modular Arithmetic

1. What is the inverse of $5 \pmod{24}$? Your answer should be a number in the set $\{0, 1, \ldots, 23\}$.

2. What is $2^{75} \pmod{35}$? Your answer should be a number in the set $\{0, 1, \ldots, 34\}$. (Hint: think about RSA with $p = 7$, $q = 5$ and $e = 5$.)

3. (8 points) Recall that RSA can also be used as a *signature scheme*. That is, we can use an RSA scheme to verify that a message actually came from the sender we expect.

   Professor Rao has created an RSA scheme with public key $(N, e) = (55, 3)$, and an unknown private key d.

   Professor Rao has sent you a message containing the answer to Question 2 on this exam (the number of TAs), but a hacker has also sent you another message trying to trick you into giving the incorrect answer. Professor Rao's message is of the form $(m, m^d \pmod{N})$, corresponding to his RSA scheme, and you'd like to verify which message actually came from Professor Rao.

   Suppose you received the messages $(12, 23)$ and $(13, 23)$. What message m did Professor Rao actually send you? Justify your answer. (Hint: Your calculations may be easier if you utilize CRT. You do not need to solve for d.)

4. If $y < x$, then $x \% y \leq x/2$. (Recall, $x \% y$ is the remainder of x divided by y; in other words, $x \% y$ is defined as $x - \lfloor x/y \rfloor \times y$.)

   ◯ True ◯ False

5. Recall that in the extended Euclidean algorithm, given $x, y \in \mathbb{Z}$ with $d = \gcd(x, y)$, we are able to find a, b such that

   $$d = ax + by.$$

   Throughout this problem, d, a, b, x, y are constants that satisfy the above equation.

   (a) Suppose i is another constant; consider the equation $zx \equiv id \pmod{y}$. What is a solution for z? (Your answer can *only* be in terms of a, b, d, and/or i.)

   (b) How many solutions for z are there to $zx \equiv id \pmod{y}$ for a fixed i?

   (c) Suppose $\gcd(x, y) = 1$. If $z \equiv i \pmod{x}$ and $z \equiv j \pmod{y}$, give an expression for $z \pmod{xy}$ using a, b, i, x, y and/or j. (Your answer may not include any unsimplified inverses.)

6. Suppose p is a prime. We will prove that for $a \not\equiv 1 \pmod{p}$, $a^k \equiv 1 \pmod{p} \implies \gcd(k, p-1) > 1$.

   (a) What is the smallest positive integer k where $2^k \equiv 1 \pmod{7}$?

   (b) (4 points) Prove that $a^k \equiv a^{k \bmod (p-1)} \pmod{p}$.

   (c) If $\gcd(k, p-1) = 1$, then $f(x) = kx \pmod{p-1}$ is a bijection from $\{1, \ldots p-1\}$ to $\{1, \ldots, p-1\}$.

   ◯ True ◯ False

(d) (8 points) Prove that if $a^k \equiv 1 \pmod{p}$, then either $\gcd(k, p-1) > 1$ or $a \equiv 1 \pmod{p}$. (Hint: Consider $a^{ki \bmod p-1}$ for $i \in \{1, \ldots p-1\}$.)

(e) Suppose $a^k \equiv 1 \pmod{p}$. If $a \not\equiv 1 \pmod{p}$, then $\gcd(k, p-1) > 1$.

◯ True ◯ False

10. Polynomials.

1. (1 point each) Working under GF(5), the polynomial that passes through the points $(0,1)$, $(1,2)$, and $(2,0)$ can be written in the form ax^2+bx+c for some coefficients a, b, and c. What are the coefficients of this polynomial? (Hint: this might be easier with linear equations rather than Lagrange.)

$a =$ $\quad$ $b =$ $\quad$ $c =$

2. Suppose we have a degree 1 polynomial $P(x)$ in GF(5). The points $(0,1)$, $(1,3)$, $(2,1)$, and $(3,2)$ are received from a communication channel that has at most 1 corruption.

   (a) What is $P(x)$?

   (b) What is the error polynomial, $E(x)$?

In the below parts, we are working under GF(p) for a sufficiently large prime p.

3. Suppose $P(x)$ is a polynomial of degree *exactly* $d > 0$, where $d < p$. What is the maximum number of points x_i such that $P(x_i) = 2$? (Your answer should be in terms of d. Recall that a polynomial is of degree exactly d if the leading coefficient $a_d > 0$.)

4. Let $P(x)$ and $Q(x)$ be polynomials of degree *exactly* d. Moreover, $P(x)$ has r distinct roots and $Q(x)$ has r' distinct roots.

   (a) What is the maximum number of distinct roots for $R(x) = P(x)Q(x)$?

   (b) What is the minimum number of distinct roots for $R(x) = P(x)Q(x)$?

(c) What is the degree of $P(x)Q(x)$?

(d) What is the maximum degree of $P(x)+Q(x)$?

5. (5 points) Prove that a polynomial $P(x)$ of degree exactly 1 has exactly 1 root.

6. We will prove that there is a polynomial of degree exactly 2 with fewer than two roots.
   If $P(x)$ has two roots, then $P(x) = a(x-r_1)(x-r_2) \pmod{p}$. Note that $P(x) = a(x-r_2)(x-r_1)$ is the same polynomial. Moreover, $P(x) = a(x-r)^2$ is considered to have two roots.

   (a) How many polynomials of degree exactly 2 are there with two roots? Recall that we are working in GF(p). (Careful: Can a be 0?)

   (b) How many polynomials of degree exactly 2 are there?

11. Rogue Delegates.

(12 points) The planning committee for The International Conference on Hackathon Organization has designed the following secret sharing scheme:

70 points of a 49-degree shared polynomial have each been assigned to the 70 delegations, one point per delegation.

Each delegation contains 10 delegates. They each receive a point of a degree 5 delegation-specific polynomial. Delegates can come together to recover their delegation's point on the shared polynomial using the delegation-specific polynomial.

A *rogue delegate* is an all-powerful delegate: they know all of the polynomials and have control over which delegation that they are placed in. The rogue delegates purposely manipulate their point on their delegation-specific polynomial to mess up the conference.

The planning committee will use the Berlekamp-Welch algorithm on the delegation-specific polynomials and on the shared polynomial to attempt to recover thestable correct secret. What is the largest number of rogue delegates that can attend the conference such that the committee is guaranteed to recover the correct secret? Justify your answer.

12. Counting.

Throughout this question, you may leave your answers unsimplified (i.e. you can leave binomial coefficients, factorials, exponents, etc. as is), but you should not use any summation or product notation (i.e. you may not use $\sum$ or $\prod$).

1. How many ways can the letters in BAA be arranged?

2. How many ways can the digits in 126 be arranged?

3. Suppose there are n teddy bears and k children, for $n > k$. How many ways are there to assign teddy bears to the children, such that every child has a single distinct teddy bear? The bears and children are both distinguishable.

4. How many ways are there to assign $x_1, \ldots, x_n \in \mathbb{N}$ (which are not necessarily distinct) such that

$$x_1 + x_2 + \cdots + x_n = k,$$

where each x_i is at least 1?

5. How many n-bit strings are there with exactly k ones?

6. How many necklaces are there with n distinguishable beads? (Note that the necklace is a circle, thus ABC is the same as CAB, if one views this as a string.)